We rank vendors based on rigorous testing and research but also take into account your feedback and our commercial agreements with providers. This page contains affiliate links.

Advertising Disclosure

How to Use the Tor Browser & Stay Safe — Full Guide 2023

Tim Mocan | **Updated on:** December 24, 2023 | Fact Checked by Hazel Shaw

Short on time? Here's how to use the Tor browser safely:

- **1. Get a Tor-friendly VPN and connect to one of its servers.** I recommend ExpressVPN, as it allows Tor traffic on all of its servers in 105 countries, has industry-leading security and privacy features, and provides fast speeds while using Tor.
- **2. Download and install the Tor browser.** Make sure to only download it from Tor's official site, otherwise you might accidentally download malicious files.
- **3. Open the Tor browser.** Wait for it to connect to the Tor network — this could take up to 10 seconds or more, depending on how fast your internet is and how overloaded the Tor network is.
- **4. Surf the web.** You can now use the Tor browser to securely access any website you want, including dark web sites.

The Tor browser is a popular way for internet users to visit dark web sites. It also provides some level of privacy and might also allow people in restrictive countries to access the free internet.

That said, the Tor browser also has some security issues, so it can't 100% protect users' privacy. Plus, some people still don't know how to get and use the Tor browser, despite it being pretty accessible and user-friendly.

So I put together this guide to show you how to use the Tor browser *and* also stay safe while doing it — in this article, I'll provide step-by-step instructions on how to install the Tor browser and surf the web with it, address Tor's security issues, give you tips on how to safely use Tor, and more.

SECURE YOUR TOR TRAFFIC WITH EXPRESSVPN

While Tor is legal in most countries, it can also be used for illegal purposes. We strongly recommend researching your local laws to make sure it's perfectly legal to use Tor and to only use it to access legal content.

Why Would You Want to Use the Tor Browser?

1. Enjoy Better Privacy

The Tor browser lets you access the Tor network, which hides your traffic and IP address — in addition, the Tor browser allows users to optionally disable website features that might compromise their privacy, although that might prevent some sites from working properly.

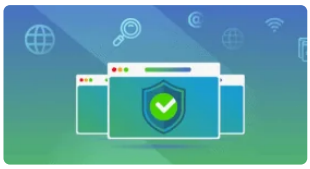
The Tor browser also prevents browser fingerprinting (the collection of data about a device or service) to a certain extent.

All of that allows internet users to enjoy a higher level of privacy when surfing the web. This way, websites and advertisers can't track their location, device information, and online preferences.

2. Circumvent Censorship

The Tor browser allows people in restrictive countries to visit blocked online services, such as social media apps, news websites, media outlets, entertainment sites, and more. Tor does that by allowing people to communicate with the internet through its servers, whose IP addresses don't have firewall restrictions linked to them.

3. Visit Dark Web Sites



This article contains

- Why Would You Want to Use the Tor Browser?
- How Does the Tor Browser Work (& Keep You Anonymous Online)?
- How to Set Up & Use the Tor Browser
- Is it Safe to Use Tor?
- How to Stay Safe While Using Tor
- Best VPNs for Accessing the Tor Network in 2023
- 🥇1. ExpressVPN — Best VPN for Accessing the Tor Network in 2023
- 🥈2. Private Internet Access — Provides Great Privacy & Security for Accessing the Tor Network
- 🥉3. NordVPN — Intuitive Apps for Surfing the Tor Network
- 4. Surfshark — Budget-Friendly & Secure VPN for Accessing the Tor Network
- 5. Proton VPN — Best Free VPN Plan for Browsing the Tor Network
- Comparison of the Best VPNs for Accessing the Tor Network in 2023
- How to Choose the Best VPN for Using the Tor Browser Safely
- What's the Difference Between the Tor Browser and a VPN?
- Tor Over VPN vs. VPN Over Tor — Which Is Safer?

Best VPN Deals

ExpressVPN — 49% Off — Get Deal

Private Internet ACCESS — 83% Off — Get Deal

CyberGhost — 84% Off — Get Deal

Some online users use the Tor browser to browse dark web sites that use .onion links, which are not available on the clearnet (the publicly accessible internet). There are tons of interesting dark web sites you can browse, including search engines, chatrooms, news sites, and even well-known platforms like Facebook.

4. Share Sensitive Information

Political activists, whistleblowers, and journalists often use the Tor browser to share information with trusted sources and protect their privacy and the privacy of their sources in the process. They use the Tor network to receive anonymous tips, investigate controversial topics, and access information that's not available on the clearnet.

5. Run Security Tests

IT staff might use the Tor network to run security tests, such as penetration testing — this involves performing an authorized cyberattack on a computer system or web application to test how secure it is.

Many hackers rely on Tor when performing cyberattacks, which is why it's often used in security tests. Running security tests using Tor allows businesses to better protect their data against threats from the dark web.

6. Ask for Medical Advice

Some people use the Tor browser to discuss their health problems with doctors over the Tor network. They likely do this because they want extra privacy and because they're not comfortable discussing their health issues with medical professionals face-to-face. Also, people who can't afford to visit a doctor or visit a clinic might use this approach as well.

7. Perform Undercover Operations

Law enforcement agents often use Tor to go undercover on the dark web, so that they can investigate and catch people who engage in illegal activities — like drug trafficking, selling illegal firearms, credit card fraud, and more.

How Does the Tor Browser Work (& Keep You Anonymous Online)?

The Tor browser is a web browser that lets you access the Tor network. The browser is free to download and use, and it's also open-source, so anyone can audit the code for security vulnerabilities.

The Tor network is a privacy network that encrypts your traffic multiple times, making it completely unreadable. When you use the Tor network to access a site, your traffic is routed through at least 3 Tor servers, which are also called "relays" or "nodes," and are usually run by volunteers. Here's a quick sketch of how a Tor connection looks:

Your Device → Tor Browser → Internet → Tor Server #1 → Tor Server #2 → Tor Server #3 → Website

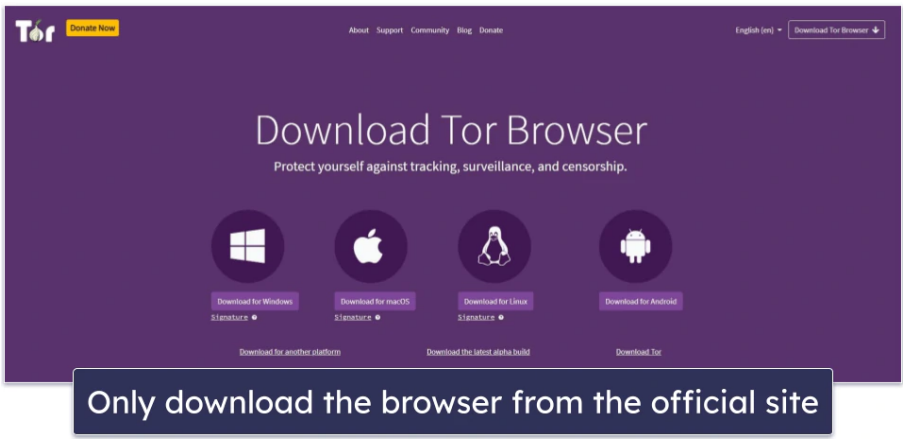
There are 4 types of Tor servers:

1. Guard servers — The first Tor server your connection goes through.
2. Middle servers — The Tor server that routes your traffic between the first and last Tor servers.
3. Exit servers — The last Tor server your connection goes through before reaching its destination (like a website, for example).
4. Bridge servers — Tor servers whose IP addresses are not made public (unlike the other types of Tor servers). These servers are intended to help people in restrictive countries circumvent censorship.

As well as encrypting your traffic, the Tor network changes your IP address — any site you access through Tor will only see the IP address of the exit Tor server, while your real IP address will remain hidden.

How to Set Up & Use the Tor Browser

1. Download & Install the Tor Browser

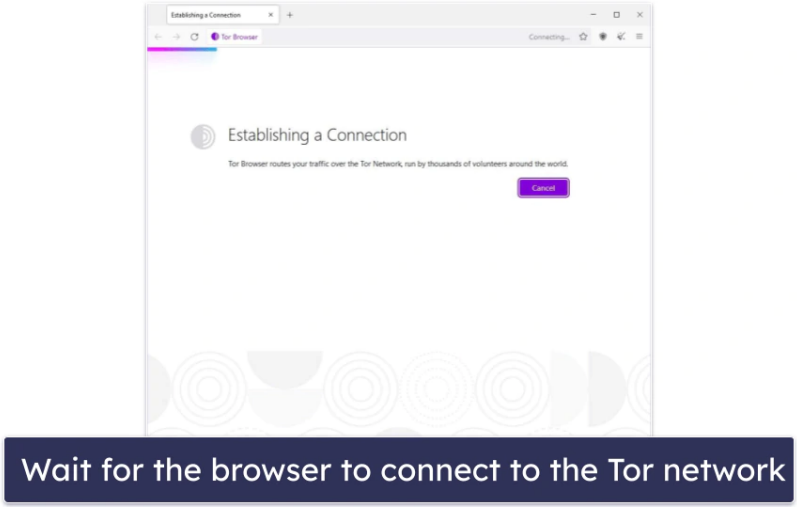


Start by downloading the Tor browser from Tor's official site. I strongly recommend avoiding unofficial sources, as you risk downloading malicious software.

The browser is available on Android, Windows, macOS, and Linux — on iOS, only the Onion Browser is available, which is a good alternative but doesn't offer as much privacy as the Tor browser. For this guide, I used the Tor browser on Windows 10.

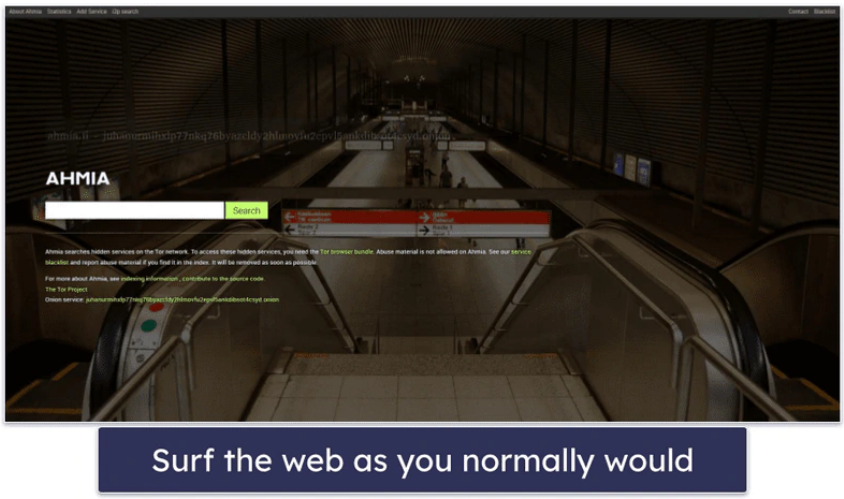
Next, open the installer and follow its instructions — installing the Tor browser won't take more than 2 minutes.

2. Open the Tor Browser


Establishing a Connection
Tor Browser
Connecting...
Establishing a Connection
Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.
Cancel
Wait for the browser to connect to the Tor network

Next, open the Tor browser app and wait for it to connect to the Tor network — this usually takes 5–10 seconds depending on how fast your internet connection is and how overloaded the Tor network is.

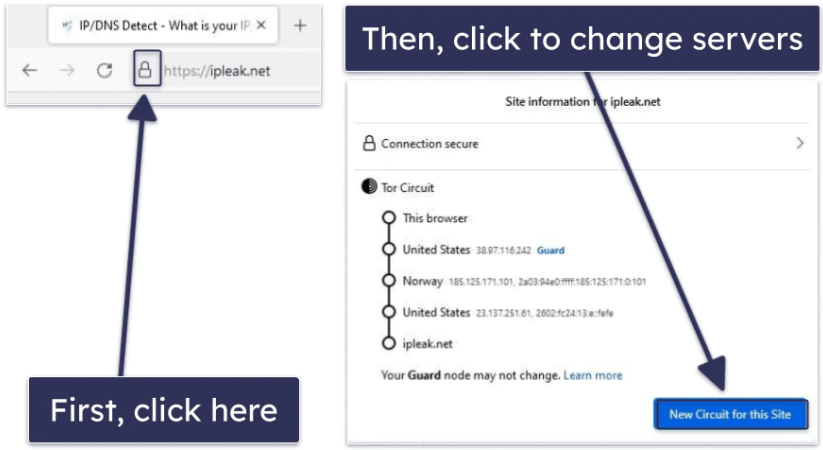
3. Connect to a Site



You can now start surfing the web while connected to the Tor network. Access any site you want as you normally would on your regular browsers. Just keep in mind it might take a bit longer to connect to a site due to Tor's slow speeds.

If you want to surf .onion sites, see our list of the best dark web sites in 2023.

4. (Optional) Change the Tor Exit Server



You can change the IP address the Tor network assigned to you by connecting to different servers — to do that, first click the padlock icon next to the site's URL bar. Next, hit the *New Circuit for This Site* button to connect to a different server chain. Repeat this process until you get an IP address from your desired country.

Is it Safe to Use Tor?

Tor generally provides good security and privacy, but it also has certain limitations and security issues:

- The guard server can see your IP address. The first Tor server you connect to can see your real IP address, which reveals your location. This is terrible for your privacy.
- Opening documents downloaded through Tor is risky. Certain documents (like PDF files) might contain internet resources that are downloaded outside of the Tor browser — this can cause your real IP address to be exposed.
- Tor doesn't encrypt all of your device's traffic. The Tor network only provides privacy as long as you use the Tor browser — if you access a site using a different browser, your IP address and data will be exposed.
- Malicious actors can run Tor servers. Pretty much anyone can run Tor servers, including hackers. Interacting with malicious Tor servers could severely compromise your privacy.
- Tor exit servers can see unencrypted traffic. If you use Tor to access HTTP websites (many dark web sites lack HTTPS), the exit server will be able to monitor your unencrypted traffic. If malicious actors are running the server, they can steal sensitive data like logins and cryptocurrency seed phrases.
- Tor has previously leaked user IP addresses. The Tor network has suffered various security issues in the past, which caused user IP addresses to leak, revealing users' real locations. Those issues have been fixed, but there's no telling when other similar security problems might pop up.
- Tor receives a lot of funding from US government agencies. This doesn't mean the US government controls Tor, but it makes it hard to fully trust Tor with protecting my privacy — after all, there's no way to know if government authorities are operating Tor servers or not.
- There are tons of malicious Tor websites. If you use Tor to access dark web sites, you're at risk of accidentally accessing malicious sites that could infect your device with malware or use scripts to compromise your privacy.

All in all, Tor provides decent security and privacy, but it's best to take precautions when using it — like using a VPN (such as ExpressVPN) to first secure your traffic before connecting to the Tor network.

How to Stay Safe While Using Tor

- Use a VPN. VPNs are online apps that change your IP address and encrypt your traffic, and I strongly recommend connecting to a VPN before you use the Tor browser — that way, your data will be secured before it reaches the Tor network. Only use a VPN that comes with essential security features, like 256-bit AES encryption, a kill switch to prevent traffic leaks, IPv6, DNS, or WebRTC leak protection, and a no-logs policy to prevent the VPN from logging your data. In my opinion, ExpressVPN is the best VPN for accessing the Tor network.
- Use an antivirus. You're likely to encounter malicious links and content on clearnet sites, so the odds of encountering them on dark web sites are even higher. That's why I recommend using Tor with an antivirus,

which is a program that can protect your device from malware infections and malicious sites — the best antivirus on the market at the moment is Norton *360*.

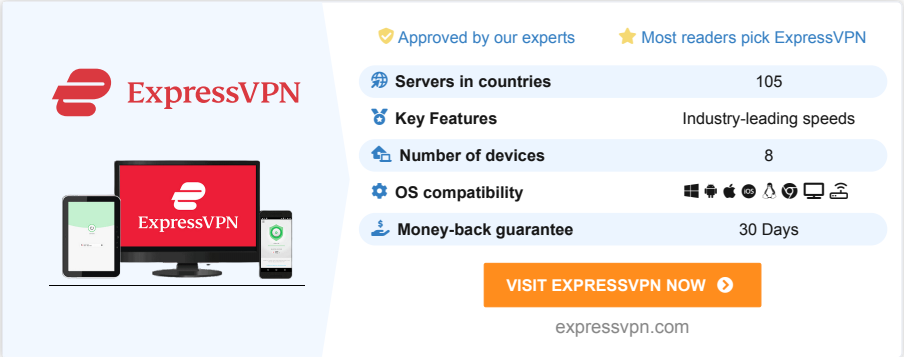
- Upgrade Tor's security levels. By default, the Tor browser's security level is set to *Standard*, which enables all website features. If you switch it to *Safer*, the browser will automatically disable website features that can be abused to endanger your privacy, like certain fonts and math symbols. And the *Safest* option disables even more site features — like JavaScript, which hackers could use to access sensitive information you shared with different sites (such as passwords).
- Use privacy-friendly search engines. Most Tor users recommend using DuckDuckGo or Startpage instead of Google, as they provide more privacy. Also, if you want to look up .onion links, I recommend using Ahmia — on top of being very accurate, it also blacklists sites that host abusive content.
- Don't access HTTP sites. If you use Tor to connect to HTTP websites, the exit servers can see your unencrypted traffic — if malicious actors are operating them, they can steal sensitive data from you. So you should only connect to HTTPS websites.
- Only access safe dark web sites. If you're using Tor to access .onion links, I strongly recommend only sticking to legit sites that are safe to use, as many shady sites could compromise your privacy and infect your device with malware.
- Don't use personal information. If you interact with dark web sites that require you to enter your name or email address, I recommend using a fake name and a secure email service (like ProtonMail) instead — otherwise, malicious actors might collect your personal data and use it to target you with cyber attacks and scams.
- Pay in cryptocurrencies. If you plan to purchase anything on the dark web (which I strongly recommend not doing), you should always use cryptocurrencies instead of credit/debit cards — they provide better privacy, and there's no risk that malicious actors will compromise your payment information.

Best VPNs for Accessing the Tor Network in 2023

Quick summary of the best VPNs for accessing the Tor network in 2023:

- 🥇**1. ExpressVPN — Best overall VPN for accessing the Tor network in 2023.** Allows Tor traffic on servers in 105 countries, provides pretty fast speeds, comes with industry-leading security and privacy features, and also has intuitive apps that make it very simple to access the Tor network with a VPN.
- 🥈**2. Private Internet Access — Provides great privacy for surfing the Tor Network.** Protects your privacy with a strict no-logs policy that has been independently audited and proven true in court and via open-source apps. Also has advanced security features, a customizable kill switch, good speeds, unlimited connections, and easy-to-use apps.
- 🥉**3. NordVPN — Intuitive apps for surfing the Tor network.** Provides easy-to-use apps for accessing the Tor network on various devices, including Windows, Android, macOS, iOS, Linux, Chrome, Android TV, and Firefox. Also comes with great security and privacy features.
- **4. Surfshark — Affordable VPN for accessing the Tor network.** Provides good speeds for surfing Tor sites and budget-friendly plans that include unlimited simultaneous connections.
- **5. Proton VPN — Best free VPN for accessing the Tor network.** The free plan allows unlimited data, allows Tor traffic on servers in 3 countries, provides decent speeds, and comes with very strong security and privacy features. The paid version adds even more servers, including Tor over VPN servers that let you surf Tor sites in browsers like Chrome.

🥇1. ExpressVPN — Best VPN for Accessing the Tor Network in 2023



ExpressVPN is my favorite VPN for accessing the Tor network — it provides excellent Tor support, has really good speeds, and comes with industry-leading security and privacy features. It's also our #1 overall VPN in 2023.

The provider allows Tor traffic on all of its servers, which are located in 105 countries — this is very convenient, as it makes it very simple to find and connect to nearby servers to get fast speeds while using the Tor network.

Speaking of speeds, ExpressVPN performed really well in my speed tests — on average, .onion links only took 5 seconds to load, and HD videos loaded in about 8 seconds and I only experienced minor buffering at the start of the videos.

ExpressVPN offers great security and privacy for accessing the Tor network — it protects your traffic with advanced security features, such as RAM-only servers (every server reset wipes all data), protection against IPv6, DNS, and WebRTC leaks, and perfect forward secrecy, which changes the encryption key for each VPN session so that hackers can't use compromised past or future keys to spy on your Tor traffic. In addition, the provider's no-logs policy has been independently audited several times, and has also been proven true in a server seizure.

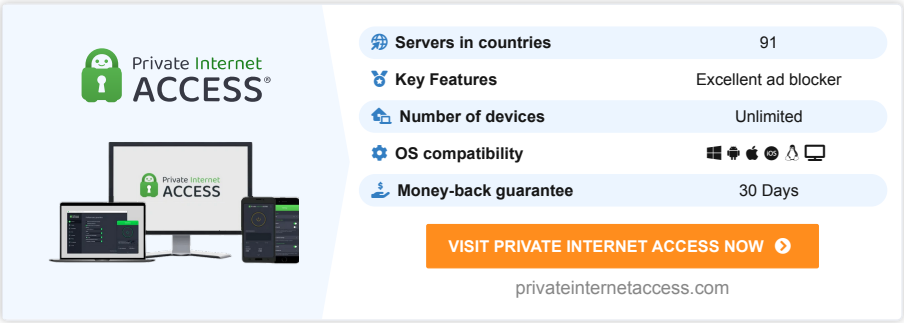
I also like that the VPN comes with split-tunneling, which lets you pick which apps use the VPN and which apps use your local network — I used this feature to only send Tor browser traffic through the VPN, which increased my speeds by about 10%.

In addition, ExpressVPN's apps are really easy to use — there's a quick-connect feature that automatically connects you to the fastest server, and the interface is very simple to navigate as well. Some apps also have Shortcuts, a feature that lets you create 1-click shortcuts for specific apps and sites that show up on your screen after connecting to the VPN. For example, you can create a shortcut for the Tor browser to instantly access it after you first secure your connection with ExpressVPN.

ExpressVPN has affordable plans that start at $6.67 / month. It also backs each purchase with a 30-day money-back guarantee.

Read our full ExpressVPN review

🥈 2. Private Internet Access — Provides Great Privacy & Security for Accessing the Tor Network



Private Internet Access (PIA) provides great security and privacy while using the Tor network. The provider's no-logs policy has been proven true in court many times — in addition, it has also passed an independent security audit. Also, all of its apps are open-source, though they're not audited like Proton VPN's apps.

PIA also secures your Tor traffic with advanced security features, including perfect forward secrecy, RAM-only servers, and full leak protection. I also like how you can configure the kill switch to disable all web access if you're not connected to a VPN server — this way, you don't accidentally risk accessing the Tor network without first securing your connection with PIA.

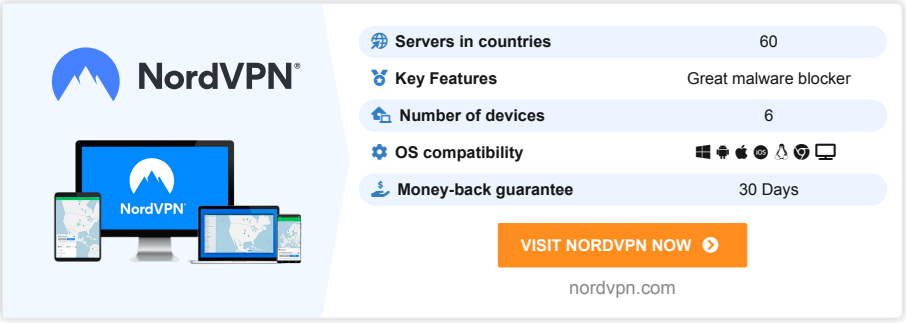
In my Tor speed tests, PIA performed pretty well — Tor sites usually took 10–12 seconds to load, HD videos loaded in less than 15 seconds and there was only minor buffering at the start and when I skipped through them. That said, the provider wasn't as fast as ExpressVPN.

I also like how simple this provider makes it to securely access the Tor network — all of its apps come with quick-connect features, make it very simple to find and connect to servers (it usually took me just 4–5 seconds to do it), and provide helpful explanations for all settings and features. Plus, I like how you can automate connections, like setting up the VPN app to automatically connect to a server when you use unsecured Wi-Fi networks to access the Tor network.

Private Internet Access has very affordable plans that start at $2.11 / month. It also backs each purchase with a 30-day money-back guarantee.

Read our full Private Internet Access review

🥉 3. NordVPN — Intuitive Apps for Surfing the Tor Network



NordVPN provides easy-to-use apps for various devices, including Windows, Android, macOS, iOS, Linux, Chrome, Android TV, and Firefox. I downloaded and installed its Android, Mac, and Windows apps in less than 2 minutes, and they were all very easy to navigate.

I'm a fan of NordVPN's Onion Over VPN servers, which route your traffic through the Tor network before it reaches the web. It's also great that you can visit .onion sites directly in your normal browser (some VPNs like Surfshark only allow you to surf .onion sites using the Tor browser).

But I don't like that the Onion Over VPN servers are only in 2 countries (Switzerland and the Netherlands). As a result, the servers are often overcrowded. I tried accessing a Tor site, and it took over 15 seconds for it to load, which is much slower than with ExpressVPN.

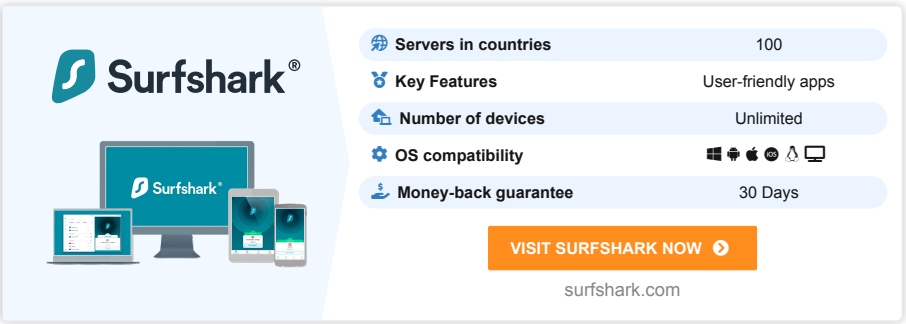
That said, NordVPN provides great security and privacy features, such as RAM-only servers, perfect forward secrecy, a strict no-logs policy that has been independently audited, and full leak protection (DNS, IPv6, and WebRTC). It also offers split-tunneling, but unlike ExpressVPN, it doesn't make this feature available for Mac. I wasn't too happy about this, because it meant I couldn't separate out my Tor traffic and send it through the VPN to increase my speeds.

I really like NordVPN's Threat Protection feature, which protects you from malicious sites and blocks ads and trackers. I tested it on some ad-heavy sites like Huffington Post and Buzzfeed, and Threat Protection blocked every single ad. As a result, Tor sites loaded faster since there were no ads to slow them down.

NordVPN has plans that start at $2.99 / month. All purchases are covered by a 30-day money-back guarantee.

Read our full NordVPN review

4. Surfshark — Budget-Friendly & Secure VPN for Accessing the Tor Network



Surfshark allows Tor traffic on all of its servers (3,200+ in 100 countries), making it really easy for you to connect to nearby servers for fast speeds while surfing Tor sites.

I tested Surfshark's speeds, and I was impressed. Tor sites and HD videos took only a few seconds to load, and I only experienced slight buffering at the start of each video.

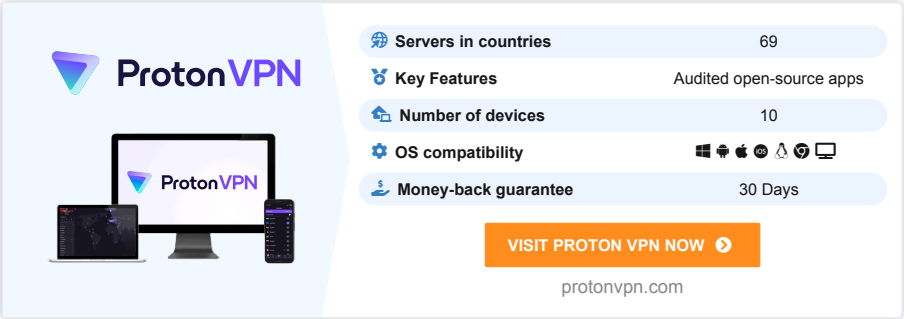
Surfshark's no-logs policy has been independently audited, and it provides some good advanced security features like split-tunneling, RAM-only servers, and perfect forward secrecy. However, the VPN doesn't offer full leak protection like ExpressVPN and Private Internet Access do (it's missing IPv6 leak protection).

I like that Surfshark allows unlimited simultaneous device connections — Private Internet Access is the only other VPN on my list to offer this. I asked everyone in my household to connect multiple devices to Surfshark at the same time, and we were all able to access the Tor network. I also like how intuitive Surfshark's apps are — I had no issues finding and connecting to a server to use the Tor browser.

Surfshark is super affordable, with plans starting at $1.99 / month. Plus, all plans come with a 30-day money-back guarantee.

Read our full Surfshark review

5. Proton VPN — Best Free VPN Plan for Browsing the Tor Network



Proton VPN has a pretty good free plan for visiting the Tor browser. This is one of the only free VPN plans on the market that has unlimited data, so you can securely surf the Tor network as much as you want. The speeds are decent, but I still experienced noticeable slowdowns — for example, it often took 15–20 seconds for a Tor site to load.

The free plan comes with excellent security and privacy features. It provides access to advanced features like full leak protection, perfect forward secrecy, and full-disk encryption, which keeps all data on a server secure even if the server is compromised. Also, the provider's no-logs policy has been independently audited, and all of its apps are open-source, meaning anyone can inspect the code for security issues — and since not all people know how to do that, I like that Proton VPN had its apps audited as well.

Unfortunately, the free plan has some limitations — it only lets you access the Tor network on servers in the US, the Netherlands, Romania, Poland, and Japan, and it limits you to 1 device. Upgrading to the paid version adds access to Tor support on 2,900+ servers in 60+ countries and faster speeds — in my tests, Tor sites loaded in 7–8 seconds, and HD videos took less than 10 seconds to load and there was minor buffering while skipping through them. The speeds are good, but ExpressVPN is still faster.

With the paid plans, you also get access to Tor over VPN servers in 5+ countries, which let you access Tor sites in regular browsers like Chrome and Opera — so you don't need to use the Tor browser at all, which is really convenient.

Proton VPN's paid plans start at $4.99 / month. There's also a 30-day money-back guarantee, but it's prorated.

Read our full Proton VPN review

Comparison of the Best VPNs for Accessing the Tor Network in 2023

VPN	Starting Price	Free Plan	Money-Back Guarantee	Number of Connections	L
🥇 **1. ExpressVPN**	**$6.67 / month**	❌	30 days	8	
🥈 **2. Private Internet Access**	**$2.11 / month**	❌	30 days	Unlimited	
🥉 **3. NordVPN**	**$2.99 / month**	❌	30 days	6	
4. Surfshark	**$1.99 / month**	❌	30 days	Unlimited	
5. Proton VPN	$4.99 / month	✅	30 days	10	

How to Choose the Best VPN for Using the Tor Browser Safely

- **Select a VPN compatible with Tor.** I tested all of the VPNs on my list and can confirm they all work with Tor 100% of the time.
- **Choose a VPN with strong security & privacy features.** Key features to look for include military-grade 256-bit encryption, a strict no-logs policy, and a kill switch that disconnects you from the internet when your connection drops to prevent your IP address from leaking on the Tor browser. You should also consider a VPN that comes with DNS leak protection for extra security.
- **Prioritize fast connection speeds.** Both Tor and VPNs inherently slow down your internet speed because they encrypt your traffic. However, with a fast VPN, you'll still be able to browse Tor with minimal interruption and shorter load times. ExpressVPN is the fastest VPN on the market.
- **Find a VPN that's easy to use & has great device compatibility.** The VPNs I recommend make it easy to find and connect to any server. Plus, they're compatible with various platforms, including Android, iOS, Windows, and macOS.
- **Consider the VPN's value.** The VPNs on my list have affordable plans, allow multiple simultaneous connections, and have money-back guarantees on all plans so you can test them risk-free.

What's the Difference Between the Tor Browser and a VPN?

	Tor Browser	VPN
Type of app	Web browser	Online app
Changes Your IP Address	✅	✅
Encrypts Your Traffic	✅ (at least 3 times)	✅ (usually just once)
Encrypts All of a Device's Web Traffic	❌ (only Tor browser traffic)	✅
Good for	Accessing dark web links, circumventing censorship, enjoying more privacy, securely sharing sensitive data as a whistleblower, activist, journalist, or undercover agent	Enjoying more online privacy, streaming, torrenting, gaming, bypassing bandwidth throttling, circumventing censorship, securely sharing sensitive data as a whistleblower, activist, journalist, or undercover agent
Free/Paid	Free	Paid, but some VPNs also have free plans

The Tor browser is a free, open-source web browser that lets you access the Tor privacy network. When you use the Tor browser, it changes your IP address and encrypts your traffic at least 3 times. The Tor browser also lets you access dark web sites, which are not available on the clearnet.

The Tor browser is mostly used to surf the dark web or evade censorship. You can also use it to enjoy better privacy online, but I honestly think a VPN is better suited for that. And you would also benefit from it if you're a journalist, whistleblower, or activist that needs to share sensitive data with their sources, or if you're an undercover agent.

A VPN is an online app that also changes your IP address and encrypts your traffic — but it only does it once, which allows VPNs to provide much faster speeds than Tor. To secure your data with a VPN, you use a VPN app (also called a VPN client) to connect to a VPN server. Once connected, the server will route and encrypt all of your internet traffic. Most top VPNs have paid subscriptions, but there are also a few providers that have good free plans that let you test their services. And unlike the Tor browser that only secures the traffic that passes through it, a VPN secures all of your device's web traffic.

Pretty much anyone stands to benefit from using a VPN. It provides great privacy and security, is good for secure streaming, torrenting, and gaming. And because VPNs encrypt your traffic but are much faster than Tor, they're also good for bypassing bandwidth throttling. Whistleblowers, journalists, and anyone else who needs to share sensitive data can also use a VPN to protect their traffic — even better, they can use it together with the Tor browser for added privacy and security.

Tor Over VPN vs. VPN Over Tor — Which Is Safer?

Tor Over VPN	VPN Over Tor
Prevents Tor from seeing your real IP address	First Tor servers always see your real IP address
Protects your real IP address if Tor leaks	Anyone can see that you're connected to the Tor network
Prevents anyone from seeing that you're using Tor	Very few VPNs support VPN over Tor connections
Most VPN providers support Tor over VPN connections	Requires a time-consuming manual setup

Easy to set up	

Tor over VPN is when you route Tor traffic over a VPN connection, so you first connect to a VPN server, and then use the Tor browser to connect to the Tor network.

Routing your VPN traffic through a Tor connection is referred to as VPN over Tor. Essentially, you initiate a connection with the Tor network via the Tor browser first, followed by a connection to a VPN server.

For the utmost privacy and security, combine Tor with a VPN connection. This encrypts your online traffic before entering the Tor network and shields your actual IP address. In case of a leak, only the VPN's IP address will be exposed.

VPN over Tor connections are pretty bad for your privacy — the first Tor server will always see your real IP address, so if a malicious actor is using it they can collect your IP and use it to track your location. And anyone (including your ISP) can see that you're connected to Tor. What's more, it's also hard to establish a VPN over Tor connection, as most VPN providers don't support them. And even if you find a VPN that does, you'll still need to perform a manual setup, which is inconvenient and time-consuming.

Frequently Asked Questions

Is it safe to download the Tor browser?

Yes, but only as long as you download it from official sources, like Tor's official website. Otherwise, you risk downloading fake apps that might infect your device with malware.

That said, using the Tor browser is not 100% safe, as the Tor network has a few security issues. That's why I strongly recommend using a VPN together with Tor to protect your privacy — all of the VPNs I mention in this article provide great Tor support and excellent privacy and security features.

Does the Tor browser hide your IP address?

Yes, but only from the sites you connect to — instead of your IP address, they will only see the IP address of a Tor server.

However, the first Tor server you connect to can see your real IP address — if a malicious actor operates it, they could collect it and use it to track your location or online behavior.

That's why I recommend using a VPN before you access Tor, as it will prevent any Tor server from seeing your real IP address — the VPNs I mentioned in this article all provide Tor support on their servers and come with very strong security and privacy features.

Does the Tor browser work on iOS?

No, but Tor devs recommend using the Onion Browser app as an alternative. It works well, it's free, and it provides decent privacy since it's open-source.

However, it can't provide the same level of privacy as the Tor browser due to how the iOS operating system works — it forces the Onion Browser app to use Apple's WebKit browser engine instead of Mozilla Firefox's Gecko browser engine, which is used by the Tor browser and can provide better anti-tracking functionality.

Does the Tor browser slow down your speeds?

Yes — I performed 10+ speed tests with Tor, and it always slowed down my original speeds by 98–99%, which is a lot. It usually took up to 5–10 seconds for most websites to load.

Tor's speeds are really slow because it encrypts your traffic multiple times. Each layer of encryption increases the time it takes for data to travel between your device, Tor's servers, and the sites you visit.

Can you use the Tor browser for torrenting?

No, as the Tor network is not good for torrenting — some Tor browsers block P2P traffic, and even Tor's developers ask users not to use the network for P2P downloads. That's because Tor's speeds are pretty slow and its bandwidth is limited, so torrenting over Tor will cause even more slowdowns. Plus, I don't think that torrenting over Tor is secure, as some Tor servers can see your IP address, which is terrible for your privacy.

Instead, I recommend using a VPN for torrenting, as you get much better P2P speeds, security, and privacy — ExpressVPN is my top pick for torrenting, as it allows P2P downloads on servers in 105 countries, has the fastest torrenting speeds out there, and provides excellent security and privacy features.

Is the Tor browser different from a VPN?

Yes — the Tor browser and a VPN are similar, but there are some differences between them. The Tor browser is a web browser that connects you to the Tor network, which changes your IP address and encrypts your traffic at least 3 times. A VPN is an online app that lets you connect to VPN servers to change your IP address and encrypt your traffic (usually just once). Also, the Tor browser is free and open-source. On the other hand, most VPNs have paid plans and only some providers have free plans, and only a few VPNs come with open-source apps.

I personally think the Tor browser is only good for surfing dark web links, while VPNs have many more use cases — they're great for streaming, torrenting, gaming, and bypassing censorship. And while both Tor and VPNs provide security and privacy, I think VPNs are better because Tor has some security issues. What's more, VPNs are much faster than Tor, and this also allows them to help you prevent bandwidth throttling.

Tor over VPN or VPN over Tor — which is better?

Tor over VPN connections are much safer than VPN over Tor connections, and easier to use too — they prevent Tor servers from seeing your real IP address, stop anyone from seeing you're using Tor, and they protect your real IP address if Tor suffers a leak. Plus, most top VPNs (like ExpressVPN) support Tor traffic on their servers.

However, VPN over Tor connections provide poor privacy, as Tor servers can collect your real IP address. What's more, anyone can see you're using the Tor network. And very few VPNs support VPN over Tor connections — and the ones that do require you to perform an inconvenient manual setup.

Best VPNs for Tor in 2023 — Final Score:

Our Rank	Provider	Our Score	Best Deal	
1	ExpressVPN	9.6	save 49%	VISIT WEBSITE >
2	Private Internet ACCESS	9.4	save 83%	VISIT WEBSITE >
3	NordVPN	9.0	save 69%	VISIT WEBSITE >
4	Surfshark	8.8	save 80%	VISIT WEBSITE >
5	ProtonVPN	8.4	save 50%	VISIT WEBSITE >

We rank vendors based on rigorous testing and research but also take into account your feedback and our commercial agreements with providers. This page contains affiliate links.

Share It:

TIM MOCAN
QA Editor

UPDATED ON: December 24, 2023

About the Author

Tim Mocan is a QA Editor at SafetyDetectives. He has 5+ years of experience researching and writing about cybersecurity topics, and he specializes in VPNs. Prior to joining SafetyDetectives, he worked as a contributor for other VPN review websites and as a content writer for several VPN providers. Throughout his freelance writing career, he has also covered other niches, including SEO, digital marketing, customer loyalty, home improvement, and health and rehab. Outside of work, Tim loves to spend his time traveling, playing video games, binging anime, and using VPNs (yes, really!).

978 904

Was this article helpful? 8 (10 votes)

SafetyDetectives

Our mission - to give our readers accurate and valuable information so they can make informed decisions about staying safe, secure and protected on the internet

© 2023 SafetyDetectives
All Rights Reserved

CATEGORIES

- Safety Blog
- Best Antivirus Software
- Best Password Managers
- Best VPN Services
- Antiviruses Coupons
- Antivirus Comparison
- News

REVIEWS

- Bitdefender Reviews
- Norton Reviews
- 1Password Reviews
- Dashlane Reviews
- ExpressVPN Reviews
- Private Internet Access Reviews

LEGAL

- Why Trust Us?
- Contact Us
- Testing Methodology
- Terms of Service
- FAQ
- Disclosure
- Privacy Policy
- DMCA Policy
- Human Sitemap
- Press Page